Panorama de Segurança, Infraestrutura de Integração RWS

RWS Ltda. · CNPJ 46.231.982/0001-23 · Av. Santo Amaro, 1047 · São Paulo/SP, Brasil

Contato de segurança: security@rwsintegration.com · Encarregado (DPO): dpo@rwsintegration.com

Versão arquivada (v2.0, Junho de 2026). A versão vigente está publicada em rwsintegration.com/pt-br/legal/security.

Este documento descreve a arquitetura de segurança, o isolamento e a conformidade da infraestrutura de integração RWS em todo o ciclo de vida dos dados: recebimento, processamento e entrega. Ele complementa o "Documento de Conformidade e Segurança: Conexão Site-to-Site", que detalha a conectividade VPN com ambientes de clientes.

SUMÁRIO

1. Data Centers e Segurança Física
2. Segurança de Rede
3. Arquitetura e Isolamento Multi-Tenant
4. Gestão de Segredos e Credenciais
5. Criptografia
6. Disponibilidade e Continuidade
7. Segurança da Aplicação (SDLC)
8. Testes de Penetração e Avaliações de Vulnerabilidade
9. Resposta a Incidentes de Segurança
10. Monitoramento, Logs e Auditoria
11. Organização e Pessoas
12. Privacidade e Proteção de Dados (LGPD)
13. Certificações e Documentação Adicional

1. Data Centers e Segurança Física

RWS

NOME	DETALHES
Instalações	A infraestrutura física da plataforma RWS é hospedada e gerenciada nos data centers seguros da Amazon Web Services (AWS). A RWS não opera servidores físicos nem data centers próprios: toda a camada física e de infraestrutura é herdada da AWS, que gerencia riscos continuamente e passa por avaliações independentes recorrentes. As operações de data center da AWS são credenciadas sob: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 1 e SOC 2 e PCI DSS. (Ver Seção 13, Certificações e Documentação Adicional.)
Segurança Física	Os data centers da AWS possuem controle de perímetro, vigilância por vídeo, sistemas de detecção de intrusão e acesso físico rigorosamente controlado, com autenticação multifator para pessoal autorizado e escolta contínua de visitantes. Detalhes públicos em aws.amazon.com/compliance/data-center/controls.
Localização	Os dados processados pela plataforma são armazenados e processados na região us-east-1 (AWS, Estados Unidos). A transferência internacional de dados ocorre sob as salvaguardas do art. 33 da LGPD (Lei 13.709/2018), por meio de cláusulas contratuais com os clientes (MSA/DPA) e dos termos de processamento de dados da AWS.

2. Segurança de Rede

NOME	DETALHES
Equipe de Resposta de Segurança	A equipe de segurança da RWS responde a alertas e eventos de segurança e pode ser contatada em security@rwsintegration.com.
Isolamento de Rede	O núcleo da plataforma é executado em uma VPC privada e isolada, sem qualquer acesso inbound a partir da internet. Todo o tráfego é exclusivamente outbound, originado pela própria plataforma (o mesmo princípio aplicado às conexões Site-to-Site). Não há exposição pública de IPs do ambiente de processamento, nem NAT reverso; as rotas de retorno são restritas a respostas de conexões iniciadas pela plataforma.
Proteção (Firewalls)	As subnets privadas são protegidas por Network ACLs e Security Groups com política de negação por padrão: apenas destinos, portas e protocolos explicitamente autorizados são permitidos, atribuídos por função de cada workload.
Endpoints Públicos	Os componentes públicos (webhooks e APIs de recepção) são expostos exclusivamente via AWS API Gateway, com autenticação, rate limiting e throttling, e tráfego protegido por HTTPS/TLS 1.2+. O componente de webhook possui autorização mínima: sua única permissão é gravar os dados recebidos na fila de extração. Não existe

NOME	DETALHES
	caminho de rede do endpoint público para o ambiente interno: a comunicação ocorre exclusivamente por filas. Mesmo em caso de abuso do endpoint público, a superfície de ataque se limita à camada de recepção.
Mitigação de DDoS	Os endpoints públicos são protegidos pelo AWS Shield Standard (mitigação automática de ataques de rede e transporte), combinado com throttling no API Gateway. O desenho assíncrono orientado a filas absorve picos de tráfego sem impacto no ambiente de processamento.
Monitoramento de Rede	O tráfego de rede é monitorado por VPC Flow Logs e CloudWatch, com alertas automáticos de anomalias.
Acesso Lógico	O acesso à rede de produção é restrito por necessidade de conhecimento (need-to-know), com contas individuais e nominais, mínimo privilégio e autenticação multifator (MFA). (Ver Seção 11, Organização e Pessoas.)

3. Arquitetura e Isolamento Multi-Tenant

NOME	DETALHES
Arquitetura	A plataforma é construída integralmente sobre serviços gerenciados e serverless da AWS (ECS Fargate, Lambda, filas e armazenamento gerenciados), operando em múltiplas zonas de disponibilidade (multi-AZ). O processamento é assíncrono e orientado a filas: falhas transitórias resultam em reprocessamento automático, não em perda de dados.
Semântica de Entrega	A plataforma garante entrega exactly-once: cada dado de integração é processado e entregue exatamente uma vez, com controle de finalização por registro; reprocessamentos automáticos não geram duplicação.
Infraestrutura como Código	O ambiente é provisionado e atualizado exclusivamente por infraestrutura como código (IaC), através de pipelines automatizados, mantendo a configuração consistente, versionada e auditável. Não há alterações manuais de infraestrutura.
Isolamento por Integração	Cada integração é executada em computação e filas totalmente isoladas. Execuções distintas não compartilham contexto de processamento.
Isolamento entre Clientes	Dados de clientes diferentes nunca se cruzam: não há reutilização de workloads, filas ou contexto entre tenants.

NOME	DETALHES
Mínimo Privilégio	As permissões de cada workload seguem o princípio do mínimo privilégio (IAM Policies), com acesso restrito exclusivamente aos recursos do próprio cliente e da própria execução.

4. Gestão de Segredos e Credenciais

NOME	DETALHES
Armazenamento	Todas as credenciais (APIs, bancos de dados, VPNs e sistemas de clientes) são armazenadas no AWS Secrets Manager, com criptografia em repouso (AES-256).
Segregação por Tenant	Cada cliente (tenant) possui um cofre próprio e segregado de segredos. Não existe repositório compartilhado de credenciais entre clientes.
Injeção em Runtime	Os segredos são injetados exclusivamente em tempo de execução no workload autorizado. Nunca são gravados em código-fonte, arquivos de configuração ou logs.
Acesso Humano	O acesso humano a segredos de clientes é restrito, auditado e não faz parte da operação diária da plataforma.

5. Criptografia

POLÍTICA	DETALHES
Criptografia em Trânsito	Toda a comunicação externa é feita por HTTPS/TLS 1.2+ (endpoints públicos e integrações via API). As conexões VPN Site-to-Site utilizam IPsec com AES-256.
Criptografia em Repouso	Os dados em repouso são criptografados com AES-256, por meio da criptografia gerenciada da AWS (SSE), em bancos de dados, filas, armazenamento de objetos e logs. A RWS não implementa criptografia proprietária: utiliza exclusivamente mecanismos criptográficos certificados e gerenciados pela AWS.
Criptografia de Backups	Os backups dos bancos de dados são realizados por snapshots automatizados, criptografados com AES-256, com período de retenção controlado. Armazenamentos transitórios de processamento (cache e filas) não retêm dados de forma durável e operam com redundância nativa dos serviços gerenciados da AWS.

6. Disponibilidade e Continuidade

RWS

POLÍTICA	DETALHES
SLA de Disponibilidade	A RWS assume contratualmente disponibilidade mensal alvo de 99,90%, com créditos de serviço (descontos progressivos sobre a assinatura) em caso de descumprimento, conforme o Formulário de Pedido. A disponibilidade é monitorada continuamente.
SLA de Processamento	Tempo-alvo de processamento dos dados de integração (recebimento → entrega) de até 15 minutos, sustentado por autoscaling automático da capacidade de processamento. Exceção: integrações com origens ou destinos sujeitos a rate limiting imposto pelo sistema externo podem exceder esse alvo, respeitando os limites do terceiro.
Redundância	Os serviços gerenciados operam em múltiplas zonas de disponibilidade (multi-AZ), eliminando pontos únicos de falha na camada de infraestrutura.
Resiliência a Falhas	O processamento orientado a filas garante que falhas transitórias resultem em reprocessamento automático, e não em perda de dados.
Recuperação de Desastres	Snapshots criptografados e retenção controlada permitem a restauração dos dados; a infraestrutura como código permite o re-provisionamento completo e consistente do ambiente.

7. Segurança da Aplicação (SDLC)

POLÍTICA	DETALHES
Revisão de Código	Todo código passa por revisão obrigatória via pull request antes de ser integrado. Não há deploy de código sem revisão.
Pipeline CI/CD	Deploys em produção ocorrem exclusivamente via pipeline automatizado (CI/CD), com portões de qualidade obrigatórios: análise estática (lint), verificação de tipos, testes automatizados e build. Credenciais de pipeline são segregadas e de mínimo privilégio.
Análise de Dependências	As dependências de terceiros são verificadas continuamente quanto a vulnerabilidades conhecidas (CVEs), com atualização priorizada por severidade. Novas versões de dependências passam por um período de quarentena antes de serem adotadas, mitigando ataques de cadeia de suprimentos (supply chain).
Segregação de Ambientes	Os ambientes de homologação e produção são totalmente segregados (credenciais, filas, bancos e computação distintos). O ambiente de homologação opera sob os mesmos controles de isolamento e acesso do ambiente de produção.

8. Testes de Penetração e Avaliações de Vulnerabilidade

RWS

POLÍTICA	DETALHES
Avaliações Internas	A RWS conduz avaliações periódicas de postura de segurança do ambiente, com base nas melhores práticas e ferramentas nativas da AWS. Os achados são classificados por risco e tratados com prioridade correspondente.
Testes de Terceiros	Testes de segurança dos serviços da RWS podem ser realizados por empresas de consultoria independentes contratadas pelo cliente, mediante autorização prévia e por escrito da RWS, conforme previsto em contrato. Os achados de cada avaliação são revisados em conjunto, classificados por risco e atribuídos à equipe responsável para resolução sob SLA. Os custos desses testes são de responsabilidade do cliente.

9. Resposta a Incidentes de Segurança

POLÍTICA	DETALHES
Processo	Em caso de incidente, a equipe de engenharia da RWS é acionada para coletar e analisar logs dos sistemas afetados (rastreamento distribuído, logs estruturados e trilhas de auditoria) e responder da forma mais apropriada. As responsabilidades entre a RWS e a AWS seguem o modelo de responsabilidade compartilhada, sob coordenação da equipe RWS.
Tempos de Resposta	Os tempos-alvo de resposta são assumidos contratualmente: incidentes críticos em até 2 horas (horário comercial) e 8 horas (finais de semana e feriados); incidentes não-críticos e solicitações de suporte em até 2 dias úteis, com créditos de serviço em caso de descumprimento.
Notificação ao Cliente	Incidentes de segurança envolvendo dados pessoais são comunicados ao cliente (Controlador) conforme o DPA e o art. 48 da LGPD, com apoio da RWS ao cliente em eventuais comunicações à ANPD.
Contato	Eventos e suspeitas de incidente podem ser reportados a security@rwsintegration.com.

10. Monitoramento, Logs e Auditoria

POLÍTICA	DETALHES
Observabilidade	A plataforma é instrumentada com rastreamento distribuído e métricas (OpenTelemetry), centralizados na stack de observabilidade da RWS.

POLÍTICA	DETALHES
Logs de Execução	Cada execução de integração gera logs estruturados, com visibilidade de erros em nível de negócio disponibilizada ao cliente na própria plataforma.
Auditoria Administrativa	Ações administrativas no ambiente AWS são auditadas via AWS CloudTrail.
Retenção	Os logs são retidos por 90 dias, com criptografia em repouso (AES-256), utilizados exclusivamente para fins de diagnóstico e suporte, com acesso restrito. Backups seguem retenção controlada por tipo de dado.

11. Organização e Pessoas

METODOLOGIA	DETALHES
Políticas de Segurança	A RWS mantém políticas internas de segurança da informação, compartilhadas com todos os colaboradores e contratados com acesso aos ativos de informação.
Treinamento	Todos os engenheiros passam por integração de segurança no onboarding, cobrindo as práticas de desenvolvimento seguro, gestão de segredos e proteção de dados (LGPD) adotadas pela plataforma, com reforço periódico.
Confidencialidade	Todos os colaboradores e contratados com acesso a informações de clientes são vinculados a acordos de confidencialidade, com obrigações equivalentes às assumidas pela RWS perante seus clientes (Seção 10 do MSA).
Acesso à Infraestrutura	A equipe não possui acesso direto ao ambiente AWS: o acesso permanente é restrito à liderança técnica (CEO e CTO), e toda alteração de infraestrutura ocorre exclusivamente via infraestrutura como código, revisada e auditável. Em incidentes, engenheiros recebem credenciais temporárias (sessões IAM com prazo definido), revogadas automaticamente ao expirar.
Controle de Acesso Corporativo	Acesso aos ambientes segue o princípio do mínimo privilégio, com contas individuais e nominais (contas compartilhadas são proibidas) e MFA obrigatório nos sistemas de administração da infraestrutura.
Revogação e Revisão	Acessos administrativos à produção são restritos à equipe de engenharia responsável pela operação e revogados imediatamente em caso de desligamento. Revisões periódicas de acesso são conduzidas pelo Security Officer da RWS.

RWS

12. Privacidade e Proteção de Dados (LGPD)

POLÍTICA	DETALHES
Papéis	A RWS atua como Operadora de dados pessoais, processando dados exclusivamente conforme as instruções e para as finalidades contratadas por seus clientes (Controladores), nos termos do MSA e do Aditivo de Tratamento de Dados Pessoais (DPA).
Encarregado (DPO)	A RWS designou Encarregado pelo Tratamento de Dados Pessoais, canal de comunicação com Titulares e com a ANPD: dpo@rwsintegration.com.
Categorias de Dados	As categorias de dados pessoais tratadas em cada integração (incluindo dados de identificação como CPF, quando aplicável) são expressamente definidas e autorizadas no Formulário de Pedido de cada cliente.
Limitação de Finalidade	O Conteúdo do Cliente é utilizado exclusivamente para fornecer e manter o serviço contratado. Dados de uso podem ser utilizados para manutenção e melhoria do serviço somente de forma agregada e desidentificada, conforme o MSA, preservadas integralmente as obrigações sobre Dados Pessoais das Leis de Proteção de Dados Aplicáveis. Os dados dos clientes nunca são comercializados nem compartilhados com terceiros, sob nenhuma forma.
Retenção e Exclusão	Ao término do contrato, o Conteúdo do Cliente é excluído em até 60 dias mediante solicitação, e as Informações Confidenciais são devolvidas ou destruídas, conforme o MSA. Durante a vigência, logs e backups seguem retenção controlada.
Transferência Internacional	Ver Seção 1 (Localização): salvaguardas do art. 33 da LGPD, cláusulas contratuais e termos de processamento da AWS.
Suboperadores	A RWS utiliza como suboperadores: AWS (hospedagem e processamento), Slack (alertas operacionais) e Google Workspace (comunicação corporativa). Alterações na lista de suboperadores são comunicadas aos clientes conforme o DPA.
Incidentes com Dados Pessoais	Comunicados conforme a Seção 9 (Resposta a Incidentes) e o art. 48 da LGPD.
Documentos Públicos	Termos de Uso: rwsintegration.com/pt-br/terms · Política de Privacidade: rwsintegration.com/pt-br/privacy

13. Certificações e Documentação Adicional

CERTIFICAÇÃO / DOCUMENTO	DETALHES
Responsabilidade Compartilhada	A segurança da plataforma segue o modelo de responsabilidade compartilhada: a AWS responde pela segurança da nuvem (infraestrutura física, rede, hipervisor), certificada pelos programas abaixo; a RWS responde pela segurança na nuvem (arquitetura, isolamento, criptografia, acesso e operação), descrita nas Seções 2 a 11 deste documento.
Certificações AWS	A infraestrutura utilizada pela RWS herda as certificações da AWS: ISO/IEC 27001 (Gestão da Segurança da Informação), ISO/IEC 27017 (Segurança em Nuvem), ISO/IEC 27018 (Proteção de Dados Pessoais em Nuvem), SOC 1 e SOC 2 (Segurança, Disponibilidade e Confidencialidade) e PCI DSS. Emitidas por organismos independentes: aws.amazon.com/compliance/programs
Testes pelo Cliente	Clientes podem contratar avaliações de segurança independentes conforme a Seção 8 (Testes de Penetração).
Documentos Disponíveis	Mediante solicitação (e NDA quando aplicável): este Panorama de Segurança, o Documento de Conformidade da Conexão Site-to-Site, o MSA/Termos Padrão, o DPA e a Política de Privacidade. Contato: security@rwsintegration.com.

Histórico de versões

Versão	Data	Alteração
3.0	Junho de 2026	Renomeada para Política de Segurança; referências ao DPA e à página de suboperadores; conteúdo dos logs de execução
2.0 (atual)	Junho de 2026	Versão publicada inicialmente sob o título Panorama de Segurança

Documentos legais

Termos de uso
Política de privacidade
Aditivo de Tratamento de Dados Pessoais (DPA)
Política de Segurança
Suboperadores

Atualizado em: Junho de 2026

Esta versão em português é a versão oficial e prevalece sobre a versão em inglês (rwsintegration.com/en/legal/security/v2.0), disponibilizada apenas por conveniência.